FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1351988-0

Total Deleted Page(s) = 3
Page 9 ~ b3; b6; b7C;
Page 10 ~ b3; b6; b7C;
Page 40 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/12/2012

To: Cyber **Attn:** CCU-2 SSA [redacted] b6 b7C

San Francisco

From: San Francisco
Squad CY2/San Jose Resident Agency
Contact: SA [redacted] b6 b7C

Approved By: [redacted] 6/13/2012

Drafted By: [redacted] :jsm b7E

Case ID #: [redacted]

Title: UNSUB(S),
UGNAZI;
GOOGLE INC. - VICTIM,
CLOUDFLARE - VICTIM,
[redacted] - VICTIM; b6 b7C
COMPUTER INTRUSION

Synopsis: To open case and subfiles.

Details: On June 8, 2012 Supervisory Special Agent (SSA) [redacted] and Special Agent (SA) [redacted] interviewed [redacted] Investigator, Trust and Safety, telephone number [redacted] email address [redacted] and [redacted] Corporate Counsel, at their place of employment, Google Inc., 1965 Charleston Road, Mountain View, California. After being advised of the identity of the interviewing Agents [redacted] provided the following information: b6 b7C

[redacted] advised that the information being provided by Google was in response to the subjects who compromised Google Accounts belonging to the company CloudFlare and their [redacted] stated that CloudFlare had also discussed this matter publicly on its blog. It appeared that on June 1, 2012, the subjects compromised the personal Google Account operated by [redacted] which was listed as the secondary email on [redacted]s Google Apps account [redacted]. The subjects used their access to the b6 b7C

UNCLASSIFIED

O&A 6/13/12 DS

O&A to SA [redacted] NTP-14 CRENT-C 6/13/2012

To: Cyber From: San Francisco
Re: [redacted] 12/06/2011 b7E

[redacted] account to obtain access to the [redacted] account, which was an administrator for cloudflare.com's Google Apps account. b6 b7C

[redacted] stated that the subjects compromised the [redacted] account by initiating Google's account recovery procedures for the account. One of the account recovery options was to receive a voice call to a recovery telephone number that the user had previously associated with the account. The voice call provides the user with a unique code that can be used to regain access to the account. b6 b7C

According to CloudFlare's blog post, the subjects instructed Google's system to send a voice call to the cell phone listed as the recovery number on the [redacted] account, [redacted] According to [redacted] on his blog, the voicemail associated with the [redacted] telephone number was compromised. [redacted] also mentioned that he received an incoming call on his cell phone from telephone number [redacted] The Google records showed that telephone number [redacted] was associated with the subjects. [redacted] advised that the subjects placed a call from [redacted] to [redacted]s cell phone shortly before the incoming voice call from Google's account recovery system thereby forcing the call from Google to the compromised voicemail box. b6 b7C

[redacted] advised that once the subjects obtained access to the [redacted] account, the subjects attempted to lock [redacted] out of the account by changing the password, secondary email address, and SMS recovery telephone number on the account. The subjects and [redacted] fought for control of the account until Google staff disabled the account and provided access to the account back to [redacted] b6 b7C

[redacted] stated that while the subjects had access to the [redacted] account, they used that access to compromise the [redacted] account by requesting that a password reset link for [redacted] be sent to the secondary email [redacted] Unlike the [redacted] account, the [redacted] account was configured to use Google's 2-step verification feature. However, a now-fixed flaw in the account recovery flow for Google Apps accounts allowed the subjects to bypass 2-step verification and compromise the [redacted] account. b6 b7C

To: Cyber From: San Francisco
Re: [redacted] 12/06/2011 b7E

Once the subjects had access to [redacted]s Google Apps account, they used that access to compromise other CloudFlare Google Apps accounts, including [redacted] According to CloudFlare, the subjects used their access to modify proxy settings for [redacted] CloudFlare published two blog posts about the incident. [redacted] said the blog posts could befound at [redacted] b6 b7C

[redacted] advised that Google's investigation found that the subjects may have compromised other Google Accounts, in addition to the [redacted] / CloudFlare accounts. In some cases, the subjects made unsuccessful recovery claims on Gmail accounts. b6 b7C

It is requested that the following subfiles be opened and assigned to SA [redacted] b6 b7C

GJ Grand Jury Materials
1AGJ Grand Jury 1A Materials

In view of the above, it is requested that a new [redacted] matter be opened and assigned to SA [redacted] b7E b6 b7C

♦♦

FD-340a (Rev. 11-12-89)

(Title) [redacted] b7E

(File No.) [redacted]

b7E

Item	Date Filed	To be returned Yes	To be returned No		Disposition
1A1				[redacted] REPORT FOR [redacted]	Digital - (Ref Serial 12)
1A2				Subscriber Info & Log in history for [redacted]	Digital (Ref Serial 14)
1A3				Subscriber Info for [redacted]	Digital (Ref Serial 17)
1A4				Subscriber Info for [redacted]	Digital (Ref Serial 18)
1A5				Subscriber Info for [redacted]	Digital (Ref Serial 19)
1A6				Subscriber Info for [redacted]	Digital (Ref Serial 20)
1A7				Subscriber Info for [redacted]	Digital (Ref Serial 21)
1A8				Subscriber Info for [redacted]	Digital (Ref Serial 22)
1A9			b3	[redacted]	Physical (Ref Serial 24)
1A10				Email from AUSA [redacted]	Digital (Ref Serial 25)
1A(11)				2 CD's containing Google account compromised info	Physical (Ref Serial 26)

b6
b7C

b7E

	Serial #	Summary	Record Type
1A1	12	(U//~~FOUO~~) Report Fo	Digital
1A2	14	(U//~~FOUO~~) Subscriber Information and Login History for	Digital
1A3	17	(U//~~FOUO~~) Subscriber information for	Digital
1A4	18	(U//~~FOUO~~) Subscriber information for	Digital
1A5	19	(U//~~FOUO~~) Subscriber Information for	Digital
1A6	20	(U//~~FOUO~~) Subscriber information for	Digital
1A7	21	(U//~~FOUO~~) Subscriber Information for	Digital
1A8	22	(U//~~FOUO~~) Subscriber Information for	Digital
1A9	24	(U//~~FOUO~~) Grand Jury Material	Digital and Physical
1A10	25	(U) Email from AUSA	Digital
1A11	26	(U) 2 compact disks containing Google account compromised information.	Physical

b6
b7C

1A(9)

FD-340 (Rev. 4-11-03)

File Number [redacted] b7E

Field Office Acquiring Evidence San Francisco / Phx

Serial # of Originating Document 24

Date Received 8/7/2012

From [redacted] b3

(Name of Contributor/Interviewee)

(Address)

(City and State)

By [redacted] b6 b7C

To Be Returned ☐ Yes ☐ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference: _____

(Communication Enclosing Material)

Description: ☑ Original notes pertaining to [redacted] b3

1A(9)

(IACII)

FD-340 (Rev. 4-11-03)

File Number [redacted] b7E

Field Office Acquiring Evidence SF

Serial # of Originating Document _____

Date Received 06/08/2012

From Google, Inc
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA [redacted] b6 b7C

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title: UNSUB(S);
UGNAZI;
GOOGLE INC - VICTIM

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

2 Compact Disks containg Google account
compromise information

(IACII)

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. [redacted] b7E

450 Golden Gate Avenue,
San Francisco, California 94102
(415) 553-7400

June 13, 2012

USA Melinda L. Haag
United States Attorney
Northern District of California
450 Golden Gate Avenue
San Francisco, California 94102

Attn: AUSA [redacted] b6 b7C
San Jose United States Attorney's Office

UNSUB(S),
UGNAZI;
GOOGLE INC. - VICTIM,
CLOUDFLARE - VICTIM,
[redacted] - VICTIM; b6
COMPUTER INTRUSION b7C

Dear USA Haag:

In June of 2012, the San Francisco Division received information from Google, Inc. regarding an investigation involving a group of individuals who compromised various Google Accounts, including accounts that belonging to the company CloudFlare and their [redacted] Google also stated b6 b7C that CloudFlare posted information regarding the compromise on their blog.

CASE PREDICATION

On approximately June 1, 2012, unknown individual(s) compromised the personal Google Account operated by [redacted] b6 b7C, which was listed as the secondary email on [redacted]s Google Apps account [redacted]. The subjects used their access to the [redacted] account to obtain access to the [redacted] account, which was an administrator for cloudflare.com's Google Apps account.

Google informed the FBI that the subjects compromised the [redacted] account by initiating Google's account b6 b7C recovery procedures for the account. One of the account recovery options was to receive a voice call to a recovery telephone number that the user had previously associated with the account.

[redacted] [redacted] b7E

The voice call provides the user with a unique code that can be used to regain access to the account.

According to CloudFlare's blog post, the subjects instructed Google's system to send a voice call to the cell phone listed as the recovery number on the [redacted] account, [redacted] According to [redacted] on his blog, the voicemail associated with the [redacted] telephone number was compromised. [redacted] also mentioned that he received an incoming call on his cell phone from telephone number [redacted] The Google records showed that telephone number [redacted] was associated with the subjects. Google advised that the subjects placed a call from [redacted] to [redacted] s cell phone shortly before the incoming voice call from Google's account recovery system, thereby forcing the call from Google to the compromised voicemail box.

Google advised that once the subjects obtained access to the [redacted] account, the subjects attempted to lock [redacted] out of the account by changing the password, secondary email address, and SMS recovery telephone number on the account. The subjects and [redacted] fought for control of the account until Google staff disabled the account and provided access to the account back to [redacted]

b6
b7C

While the subjects had access to the [redacted] account, they used that access to compromise the [redacted] account by requesting that a password reset link for [redacted] be sent to the secondary email [redacted] Unlike the [redacted] account, the [redacted] account was configured to use Google's 2-step verification feature. However, a now-fixed flaw in the account recovery flow for Google Apps accounts allowed the subjects to bypass 2-step verification and compromise the [redacted] account.

b6
b7C

Once the subjects had access to [redacted] s Google Apps account, they used that access to compromise other CloudFlare Google Apps accounts, including [redacted] According to CloudFlare, the subjects used their access to modify proxy settings for [redacted] CloudFlare published two blog posts about the incident. Google stated the blog posts could be found at [redacted]

b6
b7C

Google's investigative team also discovered that the subjects may have compromised other Google Accounts, in addition to the [redacted] / CloudFlare accounts. In some cases, the subjects made unsuccessful recovery claims on Gmail accounts.

b6
b7C

The San Francisco Division has opened a full investigation into this matter, which has been assigned to Special Agent (SA) [redacted] b6 b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge

By [redacted]
Supervisory Special Agent

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. [redacted]

450 Golden Gate Avenue
San Francisco, California 94102
(415) 553-7400

June 13, 2012

USA Melinda L. Haag
United States Attorney
Northern District of California
450 Golden Gate Avenue
San Francisco, California 94102

Attn: AUSA [redacted]
San Jose United States Attorney's Office

UNSUB(S),
UGNAZI;
GOOGLE INC. - VICTIM,
CLOUDFLARE - VICTIM,
[redacted] - VICTIM;
COMPUTER INTRUSION

Dear USA Haag:

Pursuant to the above captioned investigation, the Federal Bureau of Investigation (FBI) requests that the below listed individuals be placed on the Federal Grand Jury 6E list, in as much as they may require access to Grand Jury information during the course of the investigation:

[redacted]

[redacted] [redacted]

[redacted]

b6
b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge

[redacted]

b6
b7C

By: [redacted]
Supervisory Special Agent

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2012

On June 14, 2012, Special Agent (SA) [redacted] served a Preservation Request on [redacted] b6 b7C b7E

The Preservation Request requested all records and other evidence be preserved for 90 days [redacted] b6 b7C b7E

A copy of the preservation request, facsimile cover page and facsimile verification report are attached and made a part of this document.

Investigation on 06/14/2012 at Campbell, California

File # [redacted] b7E

Date dictated not dictated

by SA [redacted] b6 b7C

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

450 Golden Gate Avenue
San Francisco, CA 94102
(415)553-7400

June 14, 2012

[redacted] b7E

RE: Preservation Request

Dear Custodian of Records:

The Federal Bureau of Investigation (FBI) is requesting that [redacted] take all necessary steps to preserve for a period of ninety (90) days any and all records and other evidence, including, but not limited to [redacted] b6 b7C b7E

Title 18, U.S.C. §§ 2703(f) states the following:

(f) Requirement to preserve evidence -

(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The requested information relates to an ongoing, official criminal investigation. It is requested that you do not disclose the existence of the FBI's interest into this matter until you are notified that the investigation has been completed. Failure to comply with this request may subject you to criminal penalties, including, but not limited to, obstruction of justice

under Title 18 U.S.C. §§ 1503. As you are aware, disclosure could impede the investigation and interfere with the enforcement of law.

Should you have any questions or need additional information, please contact FBI Special Agent [redacted] at telephone number [redacted] b6 b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge

[redacted] b6 b7C

By [redacted]
Supervisory Special Agent

FD-448
Revised
10-27-2004

FEDERAL BUREAU OF INVESTIGATION

FACSIMILE COVER SHEET

PRECEDENCE

○ Immediate ○ Priority ◉ Routine

CLASSIFICATION

○ Top Secret ○ Secret ○ Confidential ○ Sensitive ◉ Unclassified

TO

Name of Office:	Facsimile Number:	Date:
		06/14/2012
Attn: **Online Services Custodian of Records**	Room:	Telephone Number:

FROM

Name of Office:		Number of Pages: (including cover)
FBI		**3**
Originator's Name:	Originator's Telephone Number:	Originator's Facsimile Number:
SA		**408-558-3977**

Approved:

DETAILS

Subject:
Preservation Request

Special Handling Instructions:
Please contact for any questions at or

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

TRANSMISSION VERIFICATION REPORT

TIME : 06/14/2012 16:26
NAME : CYBER CRIM
FAX : 4085583977
TEL :
SER.# : BROF0J169395

DATE,TIME	06/14 16:25
FAX NO./NAME	[redacted]
DURATION	00:00:33
PAGE(S)	03
RESULT	OK
MODE	STANDARD ECM

b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2012

On June 14, 2012, Special Agent (SA) [redacted] served a Preservation Request on [redacted] b6 b7C b7E

The Preservation Request requested all records and other evidence be preserved for 90 days for [redacted] b6 b7C b7E

A copy of the preservation request, facsimile cover page and facsimile verification report are attached and made a part of this document.

Investigation on 06/14/2012 at Campbell, California

File # [redacted] b7E

Date dictated not dictated

by SA [redacted] b6 b7C

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

450 Golden Gate Avenue
San Francisco, CA 94102
(415)553-7400

June 14, 2012

[redacted] b7E

RE: Preservation Request

Dear Custodian of Records:

The Federal Bureau of Investigation (FBI) is requesting that [redacted] take all necessary steps to preserve for a period of ninety (90) days any and all records and other evidence, including, but not limited to [redacted] b7E

[redacted] b6 b7C b7E

Title 18, U.S.C. §§ 2703(f) states the following:

(f) Requirement to preserve evidence -

(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The requested information relates to an ongoing, official criminal investigation. It is requested that you do not disclose the existence of the FBI's interest into this matter until you are notified that the investigation has been completed. Failure to comply with this request may subject you to criminal penalties, including, but not limited to, obstruction of justice under Title 18 U.S.C. §§ 1503. As you are aware, disclosure could impede the investigation and interfere with the enforcement of law.

Should you have any questions or need additional information, please contact FBI Special Agent [redacted] at telephone number [redacted] b6 b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge

b6
b7C

By [redacted]
Supervisory Special Agent

FD-448
Revised
10-27-2004

FEDERAL BUREAU OF INVESTIGATION

FACSIMILE COVER SHEET

PRECEDENCE

○ Immediate ○ Priority ◉ Routine

CLASSIFICATION

○ Top Secret ○ Secret ○ Confidential ○ Sensitive ◉ Unclassified

TO

Name of Office:	Facsimile Number:	Date:
		06/14/2012
Attn: **Compliance Team**	Room:	Telephone Number:

b7E

FROM

Name of Office:		Number of Pages: (including cover)
FBI		**3**
Originator's Name:	Originator's Telephone Number:	Originator's Facsimile Number:
SA		**408-558-3977**

b6
b7C

Approved:

DETAILS

Subject:
Preservation Request

Special Handling Instructions:
Please contact **for any questions at** **or** .

b6
b7C

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

TRANSMISSION VERIFICATION REPORT

TIME : 06/14/2012 16:25
NAME : CYBER CRIM
FAX : 4085583977
TEL :
SER.# : BROF0J169395

DATE,TIME	06/14 16:23
FAX NO./NAME	[redacted]
DURATION	00:01:22
PAGE(S)	03
RESULT	OK
MODE	STANDARD

b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2012

On June 14, 2012, Special Agent (SA) [redacted] b6 b7C served a Preservation Request on [redacted] b7E

The Preservation Request requested all records and other evidence be preserved for 90 days for [redacted] b6 b7C b7E

A copy of the preservation request, facsimile cover page and facsimile verification report are attached and made a part of this document.

Investigation on 06/14/2012 at Campbell, California

File # [redacted] b7E

Date dictated not dictated

by SA [redacted] b6 b7C

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

450 Golden Gate Avenue
San Francisco, CA 94102
(415)553-7400

June 14, 2012

[redacted] b7E

RE: Preservation Request

Dear Custodian of Records:

The Federal Bureau of Investigation (FBI) is requesting that [redacted] take all necessary steps to preserve for a period of ninety (90) days any and all records and other evidence, including, but not limited to [redacted] b6 b7C b7E

Title 18, U.S.C. §§ 2703(f) states the following:

(f) Requirement to preserve evidence -

(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The requested information relates to an ongoing, official criminal investigation. It is requested that you do not disclose the existence of the FBI's interest into this matter until you are notified that the investigation has been completed. Failure to comply with this request may subject you to criminal penalties, including, but not limited to, obstruction of justice under Title 18 U.S.C. §§ 1503. As you are aware, disclosure could impede the investigation and interfere with the enforcement of law.

Should you have any questions or need additional information, please contact FBI Special Agent [redacted] at telephone number [redacted] b6 b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge

[redacted] b6 b7C

By [redacted]
Supervisory Special Agent

FD-448
Revised
10-27-2004

FEDERAL BUREAU OF INVESTIGATION

FACSIMILE COVER SHEET

PRECEDENCE

○ Immediate ○ Priority ◉ Routine

CLASSIFICATION

○ Top Secret ○ Secret ○ Confidential ○ Sensitive ◉ Unclassified

TO

Name of Office:	Facsimile Number:	Date:
		06/14/2012
Attn: **Custodian of Records**	Room:	Telephone Number:

FROM

Name of Office:		Number of Pages: (including cover)
FBI		**3**
Originator's Name:	Originator's Telephone Number:	Originator's Facsimile Number:
SA		**408-558-3977**

Approved:

DETAILS

Subject:
Preservation Request

Special Handling Instructions:
Please contact **for any questions at** **or**

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

TRANSMISSION VERIFICATION REPORT

TIME : 06/14/2012 16:23
NAME : CYBER CRIM
FAX : 4085583977
TEL :
SER.# : BROF0J169395

DATE,TIME	06/14 16:22
FAX NO./NAME	[redacted]
DURATION	00:00:41
PAGE(S)	03
RESULT	OK
MODE	STANDARD ECM

b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2012

On June 14, 2012, Special Agent (SA) [redacted] b6 b7C b7E served a Preservation Request on [redacted]

The Preservation Request requested all records and other evidence be preserved for 90 days for [redacted] b6 b7C b7E

Investigation on 06/14/2012 at Campbell, California

File # [redacted] b7E Date dictated not dictated

by SA [redacted] b6 b7C

[redacted] b7E

[redacted] b6 b7C

A copy of the preservation request, facsimile cover page and facsimile verification report are attached and made a part of this document.

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

450 Golden Gate Ave.
San Francisco, CA 94102
(415) 553-7400
June 14, 2012

[redacted] b7E

Attention: Custodian of Records

Re: Preservation request

Dear Legal Compliance Department:

Pursuant to Title 18, United States Code, Section 2703(f) you are hereby directed to take all steps necessary to preserve all records and other evidence in the possession of [redacted] for the following:

[redacted] b6 b7C b7E

[redacted] b6 b7C b7E

Such records and evidence include, but are not limited to, [redacted] b7E

This request is made in anticipation of an appropriate Order requiring the production of all information (including content) pursuant to the Electronic Communication Transactional Records Act, 18 U.S.C. § 2701, et seq. Under Section 2703(f), you are required to preserve these items for a period of 90 days. This period is subject to renewal.

Please be advised that your failure to comply with this request may subject you to criminal penalties, including, but not limited to, obstruction of justice under 18 U.S.C. § 1503, et seq.

Because this request in being made pursuant to an official criminal investigation, you are requested not to disclose this request, or its contents to anyone.

If you have any questions or need additional information, please contact Special Agent [redacted] at telephone number [redacted] or fax number (408)558-3977. b6 b7C

Sincerely,

Stephanie Douglas
Special Agent in Charge
[redacted] b6 b7C

By: [redacted]
Supervisory Special Agent

FD-448
Revised
10-27-2004

FEDERAL BUREAU OF INVESTIGATION
FACSIMILE COVER SHEET

PRECEDENCE

○ Immediate ○ Priority ◉ Routine

CLASSIFICATION

○ Top Secret ○ Secret ○ Confidential ○ Sensitive ◉ Unclassified

TO

Name of Office:	Facsimile Number:	Date:
		06/14/2012
Attn: **Custodian of Records**	Room:	Telephone Number:

FROM

Name of Office:		Number of Pages: (including cover)
FBI		**4**
Originator's Name:	Originator's Telephone Number:	Originator's Facsimile Number:
SA		**408-558-3977**

Approved:

DETAILS

Subject:
Preservation Request

Special Handling Instructions:
Please contact for any questions at or

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

TRANSMISSION VERIFICATION REPORT

TIME : 06/14/2012 16:21
NAME : CYBER CRIM
FAX : 4085583977
TEL :
SER.# : BROF0J169395

DATE,TIME	06/14 16:20
FAX NO./NAME	[redacted]
DURATION	00:01:07
PAGE(S)	04
RESULT	OK
MODE	STANDARD

b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/18/2012

On June 11, 2012, Federal Bureau of Investigation (FBI) Staff Operations Specialist (SOS) [redacted] conducted open source searches and reviewed subscriber information provide by Google on the following email accounts: [redacted] b6 b7C

[redacted] b6 b7C

Investigation on 06/18/2012 at Campbell, California

File # [redacted] b7E

Date dictated

by SOS [redacted] b6 b7C

b6
b7C

Account [redacted] is subscribed to [redacted] is the subscriber to [redacted], email account, [redacted] Account [redacted] is subscribed to [redacted]. The secondary email address listed on all three accounts, [redacted] belongs to [redacted] Open source searches confirmed both [redacted]'s Twitter accounts were compromised on June 3, 2012 by UNDERGROUND NAZI HACKTIVIST GROUP (UGNAZI). UGNAZI tweeted telephone number [redacted] to [redacted]s followers. In addition, UGNAZI changed the SMS telephone number on [redacted]s email account to [redacted] ACS searches were negative concerning accounts [redacted]

b6
b7C

[redacted]

[redacted] b7E

[redacted] b6 b7C

Account [redacted] and [redacted] belong to [redacted] (PROTECT IDENTITY), b6 b7C b7D
date of birth [redacted] social security number [redacted]

[redacted]

[redacted] b6 b7C

[redacted] b7E

[redacted] b6 b7C

Information could not be located for account [redacted] however, [redacted] and SMS number [redacted] was identified as belonging to account [redacted] ACS searches were negative concerning [redacted] b6 b7C

[redacted] b6 b7C

Account [redacted] is associated with [redacted] account [redacted] No other information could be located on [redacted] or [redacted]. ACS searches were negative. b6 b7C

[redacted] b6 b7C

[redacted] b7E

[redacted] b6 b7C

No open source information could be located for account [redacted] ACS searches were negative. b6 b7C

[redacted]IF) (FBI) b6 b7C

From: [redacted](IF) (FBI)
Sent: Wednesday, June 27, 2012 9:52 AM
To: [redacted](IF) (FBI)
Cc: [redacted](IF) (FBI)
Subject: IC3 complaint on UGNazi and email address [redacted]@gmail.com

Classification: UNCLASSIFIED
==========

RECORD: [redacted] b7E

On 06/27/2012, MPA [redacted] forwarded the attached complaint to SA [redacted] with the New York field office and SA [redacted] and SA [redacted] with the San Francisco field office. b6 b7C
The complaint is on the Anonymous splinter group UGNazi and email address [redacted]@gmail.com.

The complaint was filed with the IC3 on 06/26/2012 by [redacted] of [redacted] telephone number [redacted] and email address [redacted]@gmail.com [redacted] reported that his gmail account was compromised on 05/12/2012 and the subjects used it to take over 23 domains he owns. He reported the subjects' domain as ugnazi.com and email address as [redacted]@gmail.com. b6 b7C

[redacted] reported he was able to recover 17 of the domains. One of the domains he was not able to recover was [redacted] which he has owned for the last 10 years and has received numerous five figure offers for. Therefore, he reported he lost $50,000. [redacted] stated the subjects transferred his domain from GoDaddy to Internet.bs. He stated he and GoDaddy have repeatedly attempted to contact Internet.bs, but they refuse to investigate [redacted] believes Internet.bs is involved with the subjects. b6 b7C

[redacted] believes the subjects are targeting high value domains since they went after his [redacted] domain and they purportedly hijacked [redacted] from another victim. b6 b7C

A search of ACS on [redacted]@gmail.com found that this email address was mentioned in San Francisco's case [redacted] [redacted] which was opened on 06/12/2012. Their case is on UGNazi, and the victims are [redacted] On 06/14/2012, San Francisco served a preservation letter to [redacted] on [redacted] along with [redacted] and many others. The case file also mentioned [redacted] 's gmail account. The IC3 received a complaint on 6/4/12 from [redacted] reported that [redacted] s twitter and gmail accounts were hacked by [redacted] along with [redacted] s website [redacted] The complaint was previously forwarded to New York and Los Angeles. San Francisco was offered the complaint was available upon request. b6 b7C b7E

New York also has an open case on UGNazi [redacted] b7E

[redacted]

Recipients were requested to advise to writer if the information is utilized in their case.

IC3 Automatch number 120402-224175.

[redacted]

b6
b7C

Management & Program Analyst
Cyber Division
Internet Crime Complaint Center (IC3)